AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for sharing a secure communication session, the method comprising:

establishing a secure socket layer (SSL) session between a client and a first server, wherein the first server publishes on a database a set of session state information for the SSL session, and wherein the SSL session state information includes:

an SSL session identifier;

a read key for encrypting communications from the client;

a write key for encrypting communications from the first server;

an encrypted running message digest; and

a message digest key which is used to encrypt the running message digest; and

wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

receiving a message from the client at a second server, wherein the message includes the SSL session identifier which identifies the SSL session between the client and the first server, and wherein the second server contains different content and performs different functions from the first server~~the client, the first server, the second server, and the database are different from one another~~;

determining that an SSL session corresponding to the received session

identifier is not configured on the second server;

querying the database with the received SSL session identifier;

retrieving from the database identifier the SSL session state information which corresponds to the received SSL session identifier and which is published by the first server;;

establishing an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

using the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server.

2-8. (Canceled).

9. (Canceled).

10. (Previously presented) The method of claim 1, wherein retrieving the running message digest includes authenticating and authorizing the first server.

11-12 (Canceled).

13. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for sharing a secure communication session, the method comprising:

establishing an SSL session between a client and a first server, wherein the first server publishes on a database a set of session state information for the SSL session, and wherein the SSL session state information includes:

an SSL session identifier;

a read key for encrypting communications from the client;

a write key for encrypting communications from the first server;

an encrypted running message digest; and

a message digest key which is used to encrypt the running message digest; and

wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

receiving a message from the client at a second server, wherein the message includes the SSL session identifier which identifies the SSL session between the client and the first server, and wherein the second server contains different content and performs different functions from the first server~~the client, the first server, the second server, and the database are different from one another~~;

determining that an SSL session corresponding to the received session identifier is not configured on the second server;

querying the database with the received SSL session identifier;

retrieving from the database the identifierSSL session state information which corresponds to the received SSL session identifier and which is published by the first server; and

establishing an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

using the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server.

14-20. (Canceled).

21. (Canceled).

22. (Previously presented) The computer-readable storage medium of claim 13, wherein retrieving the running message digest includes authenticating and authorizing the first server.

23-24 (Canceled).

25. (Currently amended) An apparatus that shares a secure communication session, comprising:

an establishing mechanism configured to establish an SSL session between a client and a first server, wherein the first server publishes on a database a set of session state information for the SSL session, and wherein the SSL session state information includes:

an SSL session identifier;

a read key for encrypting communications from the client;

a write key for encrypting communications from the first server;

an encrypted running message digest; and

a message digest key which is used to encrypt the running message digest; and

wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

a receiving mechanism configured to receive a message from the client at a second server which identifies the SSL session between the client and the first server, wherein the first message includes the SSL session identifier, and wherein the second server contains different content and performs different functions from

the first server~~the client, the first server, the second server, and the database are different from one another~~;

a determination mechanism configured to determine that an SSL session corresponding to the received session identifier is not configured on the second server;

a query mechanism configured to query the database with the received SSL session identifier;

a retrieving mechanism configured to retrieve from the database identifier the SSL session state information which corresponds to the received SSL session identifier and which is published by the first server;

a second establishment mechanism configured to establish an SSL session between the client and the second server with the same SSL session identifier based on the retrieved SSL session state information; and

a sending mechanism configured to use the running message digest to send a second message from the second server to the client through the SSL session without establishing a separate SSL session between the client and the second server.

26-32. (Canceled)

33. (Previously presented) The apparatus of claim 25, wherein the retrieving mechanism is configured to authenticate and authorize the first server prior to retrieving the running message digest.

34-35 (Canceled).